Cisco Firepower NGIPSv Quick Start Guide for VMware Deployment

Revised: November 19, 2018

You can deploy the Cisco Firepower NGIPSv for VMware using VMware. See the Cisco Firepower Compatibility Guide for system requirements and hypervisor support.

VMware Feature Support for the Firepower NGIPSv

The following table lists the VMware feature support for the Firepower NGIPSv.

Table 1 VMware Feature Support for the Firepower NGIPSv

Feature	Description	Support (Yes/No)	Comment
Cold clone	The VM is powered off during cloning.	No	–
vMotion	Used for live migration of VMs.	Yes	Use shared storage. See vMotion Guidelines, page 5.
Hot add	The VM is running during an addition.	No	–
Hot clone	The VM is running during cloning.	No	–
Hot removal	The VM is running during removal.	No	–
Snapshot	The VM freezes for a few seconds.	No	–
Suspend and resume	The VM is suspended, then resumed.	Yes	–
vCloud Director	Allows automated deployment of VMs.	No	–
VMware FT	Used for HA on VMs.	No	–

Table 1 VMware Feature Support for the Firepower NGIPSv (continued)

Feature	Description	Support (Yes/No)	Comment
VMware HA with VM heartbeats	Used for VM failures.	No	–
VMware vSphere Standalone Windows Client	Used to deploy VMs.	Yes	–
VMware vSphere Web Client	Used to deploy VMs.	Yes	–

Prerequisites for the Firepower NGIPSv and VMware

You can deploy the Firepower NGIPSv using the VMware vSphere Web Client or the vSphere standalone client on ESXi. See Cisco Firepower Threat Defense Compatibility for system requirements.

Virtual appliances use e1000 (1 Gbit/s) interfaces by default. You can replace the default interfaces with vmxnet3 or ixgbe (10 Gbit/s) interfaces.

Modify the Security Policy Settings for a vSphere Standard Switch

For a vSphere standard switch, the three elements of the Layer 2 Security policy are promiscuous mode, MAC address changes, and forged transmits. Firepower NGIPSv uses promiscuous mode to operate, and Firepower NGIPSv high availability depends on switching the MAC address between the active and the standby to operate correctly.

The default settings will block correct operation of Firepower NGIPSv. See the following required settings:

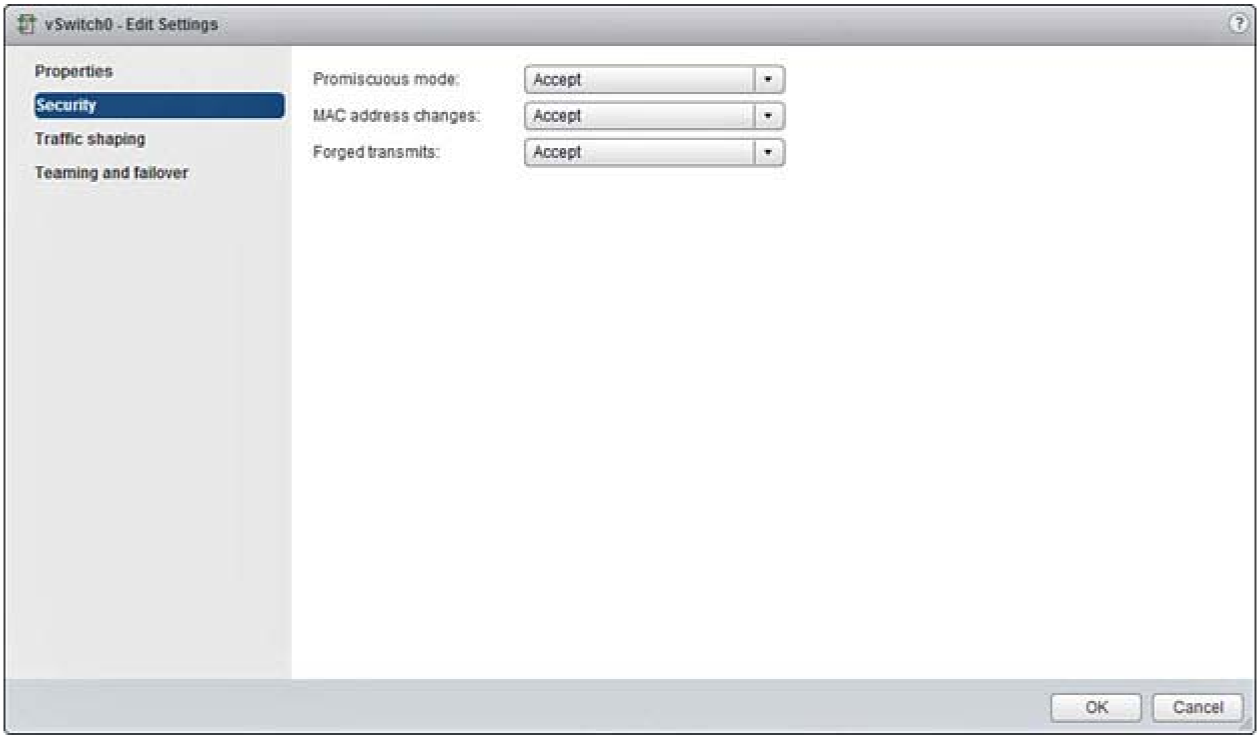
Table 2 vSphere Standard Switch Security Policy Options

Option	Required Setting	Action
Promiscuous Mode	Accept	You **must** edit the security policy for a vSphere standard switch in the vSphere Web Client and set the **Promiscuous mode** option to **Accept**. Firewalls, port scanners, intrusion detection systems and so on, need to run in promiscuous mode.
MAC Address Changes	Accept	You should verify the security policy for a vSphere standard switch in the vSphere Web Client and confirm the **MAC address changes** option is set to **Accept**.
Forged Transmits	Accept	You should verify the security policy for a vSphere standard switch in the vSphere Web Client and confirm the **Forged transmits** option is set to **Accept**.

Procedure

1. In the vSphere Web Client, navigate to the host.
2. On the **Manage** tab, click **Networking**, and select **Virtual switches**.
3. Select a standard switch from the list and click **Edit settings**.
4. Select **Security** and view the current settings.

5. **Accept** promiscuous mode activation, MAC address changes, and forged transmits in the guest operating system of the virtual machines attached to the standard switch.



Promiscuous mode: Accept

MAC address changes: Accept

Forged transmits: Accept

6. Click **OK**.

What To do Next

Ensure these settings are the same on all networks that are configured for management and failover (HA) interfaces on Firepower NGIPSv sensors.

System Requirements

The specific hardware used for Firepower NGIPSv deployments can vary, depending on the number of instances deployed and usage requirements. Each instance of the Firepower NGIPSv requires a minimum resource allocation—number of memory, CPUs, and disk space—on the server.

The following table lists the default appliance settings.

Table 3 Firepower NGIPSv Appliance Default Settings

Setting	Default	Adjustable Setting?
Memory	4GB	Yes, and for a NGIPSv you must allocate: ■ 4GB minimum ■ 5GB to use category and reputation-based URL filtering ■ 6GB to perform Security Intelligence filtering using large dynamic feeds ■ 7GB to perform URL filtering and Security Intelligence
Virtual CPUs	4	Yes, up to 8
Hard disk provisioned size	40GB	No, based on Disk Format selection
Network interfaces	2 vNICs (minimum)	Up to 10 vNICs (maximum)

Systems running VMware vCenter Server and ESXi instances must meet specific hardware and operating system requirements. For a list of supported platforms, see the VMware online Compatibility Guide.

Support for Virtualization Technology

- Virtualization Technology (VT) is a set of enhancements to newer processors that improves performance for running virtual machines. Your system should have CPUs that support either Intel VT or AMD-V extensions for hardware virtualization. Both Intel and AMD provide online processor identification utilities to help you identify CPUs and determine their capabilities.
- Many servers that include CPUs with VT support might have VT disabled by default, so you must enable VT manually. You should consult your manufacturer's documentation for instructions on how to enable VT support on your system.

Note: If your CPUs support VT, but you do not see this option in the BIOS, contact your vendor to request a BIOS version that lets you enable VT support.

Support for SSSE3

- Firepower NGIPSv requires support for Supplemental Streaming SIMD Extensions 3 (SSSE3 or SSE3S), an single instruction, multiple data (SIMD) instruction set created by Intel.
- Your system should have CPUs that support SSSE3, such as Intel Core 2 Duo, Intel Core i7/i5/i3, Intel Atom, AMD Bulldozer, AMD Bobcat, and later processors.
- See this reference page for more information about the SSSE3 instruction set and CPUs that support SSSE3.

Use the Linux Command Line to Verify CPU Support

You can use the Linux command line to get information about the CPU hardware. For example, the **/proc/cpuinfo** file contains details about individual CPU cores. Output its contents with **less** or **cat**.

You can look at the flags section for the following values:

- vmx—Intel VT extensions
- svm—AMD-V extensions
- ssse3—SSSE3 extensions

Use **grep** to quickly see if any of these values exist in the file by running the following command:

```
egrep “vmx|svm|ssse3” /proc/cpuinfo
```

If your system supports VT or SSSE3, then you should see vmx, svm, or ssse3 in the list of flags. The following example shows output from a system with two CPUs:

```
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat
pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm syscall nx lm constant_tsc pni monitor
ds_cpl vmx est tm2 ssse3 cx16 xtpr lahf_lm

flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat
pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm syscall nx lm constant_tsc pni monitor
ds_cpl vmx est tm2 ssse3 cx16 xtpr lahf_lm
```

Guidelines and Limitations for the Firepower NGIPSv and VMware

The following limitations exist when deploying Firepower NGIPSv for VMware:

- vMotion is not supported.
- Cloning a virtual machine is not supported.
- Restoring a virtual machine with snapshot is not supported.
- Restoring a backup is not supported. You cannot create or restore backup files for Firepower NGIPSv managed devices. To back up event data, perform a backup of the managing Firepower Management Center.

vMotion Guidelines

- We recommend that you only use shared storage if you plan to use vMotion. During Firepower NGIPSv deployment, if you have a host cluster you can either provision storage locally (on a specific host) or on a shared host. However, if you try to vMotion the Firepower NGIPSv to another host, using local storage will produce an error. If you do not use shared storage, the VM needs to be powered down for migration to occur.

INIT Respawning Error Messages

Symptom—You may see the following error message on the Firepower NGIPSv console running on ESXi 6 and ESXi 6.5:

```
"INIT:  Id  "ngipsv1" respawning too fast:  disabled for 5 minutes"
```

Workaround—Edit the virtual machine settings in vSphere to add a serial port while the device is powered off.

1. Right-click the virtual machine and select **Edit Settings**.
2. On the **Virtual Hardware** tab, select **Serial Port** from the **New device** drop-down menu, and click **Add**.

   The serial port appears at the bottom of the virtual device list.
3. On the **Virtual Hardware** tab, expand **Serial port**, and select connection type **Use physical serial port**.
4. Uncheck the **Connect at power on** checkbox.
5. Click **OK** to save settings.

OVF File Guidelines

You have the following installation options for installing a Firepower NGIPSv appliance:

```
Cisco_Firepower_NGIPSv_VMware-VI-X.X.X-xxx.ovf
```

```
Cisco_Firepower_NGIPSv_VMware-ESXi-X.X.X-xxx.ovf
```

where *X.X.X-xxx* is the version and build number of the file you want to use.

- If you deploy with a VI OVF template, the installation process allows you to perform the entire initial setup for Firepower NGIPSv appliance. You can specify:
  - A new password for the admin account
  - Network settings that allow the appliance to communicate on your management network
  - The detection mode
  - The managing Cisco Firepower Management Center

  Note: You must manage this virtual appliance using VMware vCenter.
- If you deploy using an ESXi OVF template, you must configure Firepower System-required settings after installation. You can manage this virtual appliance using VMware vCenter or use it as a standalone appliance; see Set Up a Firepower NGIPSv Device Using the CLI, page 10 for more information.

When you deploy an OVF template you provide the following information:

Table 4 VMware OVF Template

Setting	ESXi or VI	Action
Import/Deploy OVF Template	Both	Browse to the OVF templates you downloaded in the previous procedure to use.
OVF Template Details	Both	Confirm the appliance you are installing (Cisco Firepower Threat Defense Virtual) and the deployment option (`VI` or `ESXi`).
Accept EULA	VI only	Agree to accept the terms of the licenses included in the OVF template.
Name and Location	Both	Enter a unique, meaningful name for your virtual appliance and select the inventory location for your appliance.
Host / Cluster	Both	Select the host or cluster where you want to deploy the virtual appliance.
Resource Pool	Both	Manage your computing resources within a host or cluster by setting them up in a meaningful hierarchy. Virtual machines and child resource pools share the resources of the parent resource pool.
Storage	Both	Store all files associated with the virtual machines.
Disk Format	Both	Select the format to store the virtual disks: thick provision lazy zeroed, thick provision eager zeroed, or thin provision.
Network Mapping	Both	Select the management interface for the virtual appliance.
Properties	VI only	Customize the Virtual Machine initial configuration setup.

Deploy the Firepower NGIPSv Using the VMware vSphere Web Client or vSphere Hypervisor

You can use the VMware vSphere Web Client to deploy the Firepower NGIPSv. The Web Client requires vCenter. You can also use the vSphere Hypervisor for standalone ESXi deployment. You can use vSphere to deploy with either a VI OVF or ESXi OVF template:

- If you deploy using a VI OVF template, the appliance must be managed by VMware vCenter.
- If you deploy using a ESXi OVF template, the appliance can be managed by VMware vCenter or deployed to a standalone host. In either case, you must configure Firepower System-required settings after installation.

Before You Begin

- Download the archive file for Firepower NGIPSv from the Downloads area of the Cisco Support Site (https://software.cisco.com/ download/navigator.html).

  Note: A Cisco.com login and Cisco service contract are required.
- Unpack the archive file into a working directory. Do not remove any files from the directory.

Procedure

1. Using the vSphere Client, deploy the OVF template file you downloaded earlier by clicking **File** > **Deploy OVF Template**.
2. From the drop-down list, select one of the OVF templates you want to deploy for the Firepower NGIPSv device:

   ```
   Cisco_Firepower_NGIPSv_VMware-VI-X.X.X-xxx.ovf
   Cisco_Firepower_NGIPSv_VMware-ESXi-X.X.X-xxx.ovf
   ```

   where *X.X.X-xxx* is the version and build number of the archive file you downloaded.
3. View the OVF Template Details page and click **Next**.
4. If license agreements are packaged with the OVF template (VI templates only), the End User License Agreement page appears. Agree to accept the terms of the licenses and click **Next**.
5. Optionally, edit the name and select the folder location within the inventory where the Firepower NGIPSv will reside, and click **Next**.

   Note: When the vSphere Client is connected directly to an ESXi host, the option to select the folder location does not appear.
6. Select the host or cluster on which you want to deploy the Firepower NGIPSv and click **Next**.
7. Navigate to, and select the resource pool where you want to run the Firepower Threat Defense Virtual and click **Next**.

   Note: This page appears only if the cluster contains a resource pool.
8. Select a storage location to store the virtual machine files, and click **Next**.

   On this page, you select from datastores already configured on the destination cluster or host. The virtual machine configuration file and virtual disk files are stored on the datastore. Select a datastore large enough to accommodate the virtual machine and all of its virtual disk files.
9. Select the disk format to store the virtual machine virtual disks, and click **Next**.

   When you select **Thick Provisioned**, all storage is immediately allocated. When you select **Thin Provisioned**, storage is allocated on demand as data is written to the virtual disks. Thin provisioning can also reduce the amount of time it takes to deploy the virtual appliance.
10. For each source network specified in the OVF template, select a network by right-clicking the **Destination Networks** column in your infrastructure to set up the network mapping for each Firepower NGIPSv interface and click **Next**.

    Ensure the Management interface is associated to a VM Network that is reachable from the Firepower Management Center. Non-management interfaces are configurable from the Firepower Management Center.

    The networks may not be in alphabetical order. If it is too difficult to find your networks, you can change the networks later. After you deploy, right-click the Firepower NGIPSv instance, and choose **Edit Settings** to access the **Edit Settings** dialog box. However that screen does not show the Firepower NGIPSv interface IDs (only Network Adapter IDs).

See the following concordance of Network Adapter, Source Networks and Destination Networks for Firepower NGIPSv interfaces:

Table 5 Source to Destination Network Mapping

Network Adapter	Source Networks	Destination Networks	Function
Network adapter 1	Management	Management0/0	Management
Network adapter 2	Internal	GigabitEthernet0/0	Inside data
Network adapter 3	External	GigabitEthernet0/1	Outside data

After you deploy the Firepower NGIPSv, you can optionally return to the vSphere Client to add extra interfaces from the **Edit Settings** dialog box. You can have a total of 10 interfaces when you deploy a Firepower NGIPSv device. For data interfaces, make sure that the **Source Networks** map to the correct **Destination Networks**, and that each data interface maps to a unique subnet or VLAN. For more information, see the vSphere Client online help.

11. If user-configurable properties are packaged with the OVF template (VI templates only), set the configurable properties and click **Next**.

12. Review and verify the settings on the **Ready to Complete** window. Optionally, check the **Power on after deployment** option to power on the Firepower NGIPSv, then click **Finish**.

    After you complete the wizard, the vSphere Web Client processes the VM; you can see the “Initialize OVF deployment” status in the **Global Information** area **Recent Tasks** pane.

    When it is finished, you see the Deploy OVF Template completion status.

    The Firepower NGIPSv VM instance then appears under the specified data center in the Inventory. Booting up the new VM could take up to 30 minutes.

    Note: To successfully register the Firepower NGIPSv with the Cisco Licensing Authority, the Firepower NGIPSv requires Internet access. You might need to perform additional configuration after deployment to achieve Internet access and successful license registration.

What To Do Next

- Determine if you need to modify the virtual appliance’s hardware and memory settings, or configure interfaces; see Post-Installation Configuration, page 8.
- Register your Firepower Threat Defense Virtual to a Firepower Management Center; see Register a Firepower NGIPSv to a Firepower Management Center, page 13.

Post-Installation Configuration

After you deploy a virtual appliance, confirm that the virtual appliance’s hardware and memory settings meet the requirements for your deployment (see System Requirements, page 3). Do **not** decrease the default settings, as they are the minimum required to run the system software.

Verifying Virtual Machine Properties

Use the VMware Virtual Machine Properties dialog box to verify the host resource allocation for the selected virtual machine. You can view CPU, memory, disk, and advanced CPU resources from this tab. You can also change the power-on connection setting, the MAC address, and the network connection for the virtual Ethernet adapter configuration for a virtual machine.

Procedure

1. Right-click the name of your new virtual appliance, then select **Edit Settings** from the context menu, or click **Edit virtual machine settings** from the **Getting Started** tab in the main window.
2. Make sure the **Memory**, **CPUs**, and **Hard disk 1** settings are set to the defaults, as described in Table 3 Firepower NGIPSv Appliance Default Settings, page 4.

   The memory setting and the number of virtual CPUs for the appliance are listed on the left side of the window. To see the hard disk **Provisioned Size**, click **Hard disk 1**.
3. Confirm the **Network adapter 1** settings are as follows, making changes if necessary:
   a. Under **Device Status**, enable the **Connect at power on** check box.
   b. Under **MAC Address**, manually set the MAC address for your virtual appliance's management interface.

      Manually assign the MAC address to your virtual appliance to avoid MAC address changes or conflicts from other systems in the dynamic pool.

      Additionally, for virtual Cisco Firepower Management Centers, setting the MAC address manually ensures that you will not have to re-request licenses from Cisco if you ever have to reimage the appliance.
   c. Under **Network Connection**, set the **Network label** to the name of the management network for your virtual appliance.
4. Click **OK**.

What to Do Next

- Initialize the virtual appliance; see Initializing a Virtual Appliance, page 10.
- Optionally, before you power on the appliance, you can replace the default e1000 interfaces with vmxnet3 interfaces, create an additional management interface, or both; see Adding and Configuring VMware Interfaces, page 9.

Adding and Configuring VMware Interfaces

VMware defaults to e1000 (1 Gbit/s) interfaces when it creates a virtual machine. Once the virtual machine is finished and the Firepower NGIPSv is installed fully you can switch from the e1000 to vmxnet3 (10 Gbit/s) interfaces for greater network throughput. The following guidelines are important when replacing the default e1000 interfaces:

- You can replace the default e1000 (1 Gbit/s) interfaces with vmxnet3 (10 Gbit/s) interfaces by deleting all of the e1000 interfaces and replacing them with vmxnet3 interfaces.
- For vmxnet3, Cisco recommends using a host managed by VMware vCenter when using more than four vmxnet3 network interfaces. When deployed on standalone ESXi, additional network interfaces are not added to the virtual machine with sequential PCI bus addresses. When the host is managed with a VMware vCenter, the correct order can be obtained from the XML in the configuration CDROM. When the host is running standalone ESXi, the only way to determine the order of the network interfaces is to manually compare the MAC addresses seen on the Firepower NGIPSv to the MAC addresses seen from the VMware configuration tool.
- Although you can mix interfaces in your deployment (such as, e1000 interfaces on a virtual Cisco Firepower Management Center and vmxnet3 interfaces on its managed virtual device), you cannot mix interfaces on the same appliance. **All sensing and management interfaces on the appliance must be the same, either e1000 or vmxnet3**.

To replace e1000 interfaces with vmxnet3 interfaces, use the vSphere Client to first remove the existing e1000 interfaces, add the new vmxnet3 interfaces, and then select the appropriate adapter type and network connection.

You can also add a second management interface on the same virtual Firepower Management Center to manage traffic separately on two different networks. Configure an additional virtual switch to connect the second management interface to a managed device on the second network. Use the vSphere Client to add a second management interface to your virtual appliance.

Note: Make all changes to your interfaces **before** you turn on your appliance. To change the interfaces, you must un-register from the Firepower Management Center, power down the appliance, delete the interfaces, add the new interfaces, power on the appliance, and then re-register to the Firepower Management Center.

For more information about using the vSphere Client, see the VMware website (http://vmware.com). For more information about multiple management interfaces, see “Managing Devices” in the *Firepower Management Center Configuration Guide*.

Initializing a Virtual Appliance

After you install a virtual appliance, initialization starts automatically when you power on the virtual appliance for the first time.

Caution: Startup time depends on a number of factors, including server resource availability. It can take up to 40 minutes for the initialization to complete. Do not interrupt the initialization or you may have to delete the appliance and begin again.

Use the following procedure to initialize a virtual appliance.

Procedure

1. Power on the appliance. In the vSphere Client, right-click the name of your imported virtual appliance from the inventory list, then select **Power** > **Power On** from the context menu.
2. Monitor the initialization on the VMware console tab.

What to Do Next

- If you used a VI OVF template and configured your Firepower System-required settings during deployment, no further configuration is required; see Register a Firepower NGIPSv to a Firepower Management Center, page 13.
- If you used an ESXi OVF template or you did not configure Firepower System-required settings when you deployed with the VI OVF template, continue with Set Up a Firepower NGIPSv Device Using the CLI, page 10.

Set Up a Firepower NGIPSv Device Using the CLI

Because Firepower Threat Defense Virtual appliances do not have web interfaces, you must set up a virtual device using the CLI if you deployed with an ESXi OVF template. You can also use the CLI to configure Firepower System-required settings if you deployed with a VI OVF template and did not use the setup wizard during deployment.

Note: If you deployed with a VI OVF template and used the setup wizard, your virtual device is configured and no further action is required.

When you first log into a newly configured device, you must read and accept the EULA. Then, follow the setup prompts to change the administrator password, and configure the device’s network settings and detection mode.

When following the setup prompts, for multiple-choice questions, your options are listed in parentheses, such as `(y/n)`. Defaults are listed in square brackets, such as `[y]`. Press Enter to confirm a choice.

Note that the CLI prompts you for much of the same setup information that a physical device’s setup web page does. For more information, see the *Firepower System Installation Guide*.

Note: To change any of these settings for a virtual device after you complete the initial setup, you must use the CLI. For more information, see the Command Line Reference chapter in the *Firepower Management Center Configuration Guide*.

Understanding Device Network Settings

The Firepower System provides a dual stack implementation for both IPv4 and IPv6 management environments. You must set the IPv4 or IPv6 management IP address, netmask or prefix length, and default gateway. You can also specify up to three DNS servers, as well as the host name and domain for the device. Note that the host name is not reflected in the syslog until after you reboot the device.

Understanding Detection Modes

The detection mode you choose for a virtual device determines how the system initially configures the device’s interfaces, and whether those interfaces belong to an inline set or security zone. The detection mode is not a setting you can change later; it is simply an option you choose during setup that helps the system tailor the device’s initial configurations. In general, you should choose a detection mode based on how your device is deployed.

Passive

Choose this mode if your device is deployed passively, as an intrusion detection system (IDS). In a passive deployment, virtual devices can perform network-based file and malware detection, and Security Intelligence monitoring, as well as network discovery.

Inline

Choose this mode if your device is deployed inline, as an intrusion prevention system (IPS).

Note: Although general practice in IPS deployments is to fail open and allow non-matching traffic, inline sets on virtual devices lack bypass capability.

Access Control

Choose this mode if your device is deployed inline as part of an access control deployment, that is, if you want to perform application, user, and URL control. A device configured to perform access control usually fails closed and blocks non-matching traffic. Rules explicitly specify the traffic to pass.

In an access control deployment, you can also perform advanced malware protection, file control, Security Intelligence filtering, and network discovery.

Network Discovery

Choose this mode if your device is deployed passively, to perform host, application, and user discovery only.

The following table lists the interfaces, inline sets, and zones that the system creates depending on the detection mode you choose.

Table 6 Initial Configurations Based on Detection Mode

Detection Mode	Security Zones	Inline Sets	Interfaces
Inline	Internal and External	Default Inline Set	First pair added to Default Inline Set–one to the Internal and one to the External zone
Passive	Passive	None	First pair assigned to Passive zone
Access Control	None	None	None
Network Discovery	Passive	None	First pair assigned to Passive zone

Note that security zones are a Firepower Management Center-level configuration which the system does not create until you actually add the device to the Firepower Management Center. At that time, if the appropriate zone (Internal, External, or Passive) already exists on the Firepower Management Center, the system adds the listed interfaces to the existing zone. If the zone does not exist, the system creates it and adds the interfaces. For detailed information on interfaces, inline sets, and security zones, see the *Firepower Management Center Configuration Guide*.

Procedure

1. Open the VMware console.
2. Log into the virtual appliance at the VMware console using `admin` as the username and the new admin account password that you specified in the deployment setup wizard.

   If you did not change the password using the wizard or you are deploying with a ESXi OVF template, use `Admin123` as the password.

   The device immediately prompts you to read the EULA.
3. Read and accept the EULA.
4. Change the password for the `admin` account. This account has the Configuration CLI access level, and cannot be deleted.

   Note: Cisco recommends that you use a strong password that is at least eight alphanumeric characters of mixed case and includes at least one numeric character. Avoid using words that appear in a dictionary.
5. Configure network settings for the device. First configure (or disable) IPv4 management settings, then IPv6. If you manually specify network settings, you must:

   – Enter IPv4 addresses, including the netmask, in dotted decimal form. For example, you could specify a netmask of `255.255.0.0`.

   – Enter IPv6 addresses in colon-separated hexadecimal form. For an IPv6 prefix, specify the number of bits; for example, a prefix length of `112`.

   The VMware console may display messages as your settings are implemented.
6. Specify the detection mode based on how you deployed the device.

   The VMware console may display messages as your settings are implemented. When finished, the device reminds you to register this device to a Cisco Firepower Management Center, and displays the CLI prompt.
7. Verify the setup was successful when the console returns to the firepower **#** prompt.

   Note: To successfully register the Firepower NGIPSv with the Cisco Licensing Authority, the Firepower NGIPSv requires Internet access. You might need to perform additional configuration after deployment to achieve Internet access and successful license registration.

What to Do Next

- Register your Firepower NGIPSv to a Firepower Management Center; see Register a Firepower NGIPSv to a Firepower Management Center, page 13.

Register a Firepower NGIPSv to a Firepower Management Center

Because virtual devices do not have web interfaces, you must use the CLI to register a virtual device to a Cisco Firepower Management Center, which can be physical or virtual. It is easiest to register a device to its Firepower Management Center during the initial setup process, because you are already logged into the device's CLI.

To register a device, use the `configure manager add` command. A unique self-generated alphanumeric registration key is always required to register a device to a Firepower Management Center. This is a simple key that you specify, and it is not the same as a license key.

In most cases, you must provide the Firepower Management Center's IP address along with the registration key, for example:

```
configure manager add XXX.XXX.XXX.XXX my_reg_key
```

where *XXX.XXX.XXX.XXX* is the IP address of the managing Firepower Management Center and *my_reg_key* is the registration key you entered for the virtual device.

Note: On the ESXi platform, when using the vSphere Client to register a virtual device to a Firepower Management Center, you must use the IP address (not the hostname) of the managing Firepower Management Center if DNS information is not provided during the setup.

However, if the device and the Firepower Management Center are separated by a Network Address Translation (NAT) device, and the Firepower Management Center is behind a NAT device, enter a unique NAT ID along with the registration key, and specify `DONTRESOLVE` instead of the IP address. For example:

```
configure manager add DONTRESOLVE my_reg_key my_nat_id
```

where *my_reg_key* is the registration key you entered for the virtual device and *my_nat_id* is the NAT ID of the NAT device.

If the device, rather than the Firepower Management Center, is behind a NAT device, enter a unique NAT ID along with the registration key, and specify the host name or IP address of the Firepower Management Center. For example:

```
configure manager add [hostname | ip address] my_reg_key my_nat_id
```

where *my_reg_key* is the registration key you entered for the virtual device and *my_nat_id* is the NAT ID of the NAT device.

Procedure

1. Log into the virtual device as a user with CLI Configuration (Administrator) privileges:
   - If you are performing the initial setup from the VMware console, you are already logged in as the `admin` user, which has the required access level.
   - Otherwise, log into the device using the VMware console, or, if you have already configured network settings for the device, SSH to the device's management IP address or host name.
2. At the prompt, register the device to a Cisco Firepower Management Center using the `configure manager add` command, which has the following syntax:

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} reg_key
[nat_id]
```

where:

- {*hostname* | *IPv4_address* | *IPv6_address* | DONTRESOLVE} specifies the IP address of the Firepower Management Center. If the Firepower Management Center is not directly addressable, use DONTRESOLVE.
- *reg_key* is the unique alphanumeric registration key required to register a device to the Firepower Management Center.

Note: The registration key is a user-generated one-time use key that must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). You will need to remember this registration key when you add the device to the Firepower Management Center.

- *nat_id* is an optional alphanumeric string used during the registration process between the Cisco Firepower Management Center and the device. It is required if the hostname is set to DONTRESOLVE.

Note: Use the `show managers` command to monitor the state of the device registration.

3. Log out of the appliance.

What to Do Next

- Log into its web interface and use the Device Management (**Devices** > **Device Management**) page to add the device if you have already set up the Firepower Management Center. For more information, see the Managing Devices chapter in the *Firepower Management Center Configuration Guide*.